REMARKS/ARGUMENTS

The Applicant has amended claims to clarify that which the Applicant considers to be the invention. The Applicant respectfully submits that amendments to the claim set is fully supported by the originally filed specification.

Claim 14 has been amended to render claim 14 an independent claim to a system. Dependent claims 15-27 are unchanged and depend from independent system claim 14. Authentication protocol claims 1-13 are unchanged. It is respectfully submitted that this amendment addresses the objection under 35 CFR 1.75(c). Claim 14 has also been amended for clarity and imports certain features from original claim 1. Amended claim 14 is fully supported by reference to original claim 1 and original claim 14 and furthermore by reference to Fig. 6 and the associated description in the specification beginning at page 47.

In relation to the double patenting rejection a terminal disclaimer is filed in compliance with 37 CFR 1.321(c).

At pages 3-7 of the Office Action, the Examiner rejects claims 1-5, 8-11, 13-18, 21-24 and 27 under 35 USC 102(b) as being anticipated by Bjerrum *et al.* (US 5,311,595). A claim is only anticipated if all of its limitations are present in a single reference in the prior art. Because all of the limitations of the claims in the present invention are not present in Bjerrum *et al.*, as discussed below, the present invention is not anticipated by Bjerrum *et al.* and the rejection is respectfully traversed. Reconsideration and withdrawal of the rejection is requested.

Bjerrum *et al.* discloses a method of transferring data, an electronic document or the like from a first computer system to a second computer system, this prior art document is not directed to a consumable authentication protocol for validating the authenticity of an untrusted authentication chip. Rather, Bjerrum *et al.* seeks to establish secure data or document transfer between two computer systems without having to exchange encryption/decryption keys between the systems (col. 2, lines 9-12). Bjerrum *et al.* discloses the requirement to verify that data transferred from the first computer system is identical to the data received at the second computer system (col. 12, lines 35-40). This is a different object of invention to the present invention as defined in independent claims 1 and 14 of the present application. The present invention is not concerned with integrity of transmitted data to which the invention of Bjerrum *et al.* is directed.

It is respectfully submitted that there is little material overlap between Bjerrum *et al.* and the presently claimed invention as defined in either claim 1 or claim 14. In Bjerrum *et al.* the data is processed exclusively by the electronic card 124 and card 224 (col. 13, lines 12-13). To facilitate transfer of data between the cards 124 and 224, the cards must be issued together and constitute a coherent set of cards being pre-programmed as regards encryption/decryption algorithms and keys in such a way that the cards are able to communicate with each other (col. 13, lines 23-30). An authenticity verification can be made between the two electronic cards 124 and 224 prior to data transfer (col. 13, lines 62-64). However, the authenticity/integrity verification, which is characteristic of the invention, is implemented with an integrated circuit card constituting a combination of a station and an electronic card such as a combination of a station 122 and the card 124 (col. 14, lines 41-47). The printed circuit card 160 or 260 thus constitutes a complimentary card relative to the second printed circuit card or relative to an electronic card for use in connection with an associated station (col. 14, lines 49-53). Hence, authentication requires a complimentary

electronic device to interact with the electronic card 124 and 224. Such a requirement is not necessary in the presently claimed invention.

Bjerrum *et al.* also discloses use of a security module or security terminal being a tamper-proof station, that is, stations that due to their physical design make it impossible to open the system and reveal material as well as software (col. 14, lines 63-68). It is precisely this requirement of physical security dependence that the present invention seeks to avoid.

The Examiner relies on disclosure in parts of col. 4 and 5 and col. 25, line 25 to col., 26 line 7 to anticipate the presently claimed invention. However, it is respectfully submitted that upon a correct construction of the features of the present invention, as defined in either claim 1 or claim 14, no disclosure of the complete method or system is found in Bjerrum *et al.* The Applicant respectfully submits that the generalised use of encryption/decryption disclosed in Bjerrum *et al.* does not anticipate the specific and distinct features of the presently claimed invention.

Referring to claim 1 of the present application, with reference to the preferred embodiment illustrated in Fig. 4, a random number R is generated and an asymmetric encrypt function E_{KT} is applied to the random number using a first key to produce a first outcome 61. The first outcome produced in trusted chip 23 is passed 62 to the untrusted authentication chip. The first outcome is decrypted with an asymmetric decrypt function using a secret key to produce a second outcome in the untrusted chip 20. The asymmetric encrypt function is applied to the second outcome together with a data message read from the untrusted chip 20 using the secret key to produce a third outcome 63 in the untrusted chip 20. The third outcome is decrypted and compared to the decrypted random number and data message with the generated random number R and the received data message. This series of protocol steps is very different to the references relied upon by the Examiner in Bjerrum *et al.*

In the present invention, the public key K_T is in trusted chip 23, while the secret key K_A is in untrusted chip 20. Having K_T in trusted chip 23 has the advantage that trusted chip 23 can be implemented in software or hardware, by using a random number R that is seeded with a different random number for each system. Such an advantage is not suggested by the invention of Bjerrum *et al.*

In the present invention, only a valid untrusted chip 20 would know the value of R since R is not passed into an authenticate function (it is passed in as an encrypted value). Random number R is obtained by decrypting E [R], which can only be done using the secret key K_A. Once obtained, R is appended to message M and then the result is re-encoded. Trusted chip 23 can then verify that the decoded form of E_{KA} [R/M] equals R/M and hence untrusted chip 20 is valid. This is not what is disclosed or suggested in Bjerrum *et al.*

This affords the present invention numerous advantages, for example, the secret key K_A is not revealed during the authentication process, and also, given E_{KT} [X], a clone chip cannot generate X without K_A or access to a real chip. Furthermore, since the trusted chip and untrusted chip contain different keys, testing of the trusted chip will reveal nothing about the secret key K_A. Still furthermore, even if the system of the present invention could be rewired so that the untrust d chip requests were directed to the trusted chip, the trusted chip could never answer for the untrusted chip since K_T is not equal to K_A. These advantages highlight significant differences and advantages over Bjerrum *et al.*

Nowhere is such an authentication protocol or system disclosed, taught or suggested in Bjerrum *et al.* for at least aforementioned reason, it is respectfully submitted that independent claims 1 and 14 of the present application are not anticipated by or obvious in light of Bjerrum *et al.* or the other prior art documents of record. Likewise, the dependent claims of the present application are respectfully submitted to be patentable over Bjerrum *et al.* when taken individually or in combination with any of the other prior art documents of record.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC 102(b) and 35 USC 103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762